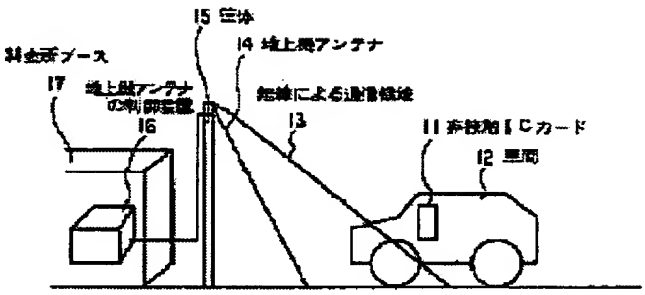
NONCONTACT IC CARD SYSTEM

Patent number: JP8221624
Publication date: 1996-08-30
Inventor: KATO MASAKI; FUJITA ICHIRO; YAMAMOTO KIMIYUKI
Applicant: MITSUBISHI HEAVY IND LTD
Classification:
- international: G07B15/00; G07B15/00; G06K17/00; G07F7/08; G08G1/017
- european:
Application number: JP19950028134 19950216
Priority number(s):

Abstract of **JP8221624**

PURPOSE: To provide a noncontact IC card which can maintains the security on a radio line with a ground equipment antenna.
CONSTITUTION: As for the noncontact IC card system of toll reception system which allows vehicles to travel on a toll highway on a non-stop and cashless basis, a noncontact IC card 11 consists a ciphering algorithm execution unit for message ciphering and a secret key storage memory for ciphering, and the ground equipment antenna 14 also consists of a ciphering algorithm execution unit and a secret key storage memory for ciphering, and messages sent from both the noncontact IC card 11 and ground equipment antenna 14 are ciphered, key numbers are also sent as the contents of the messages at the same time, and keys for ciphering are updated, message by message, to improve the secrecy of exchanged messages.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－221624

(43)公開日　平成８年(1996)８月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０７Ｂ　15/00	５１０		Ｇ０７Ｂ　15/00	５１０	
				Ｇ	
				Ｊ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｌ	
				Ｆ	

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平7－28134

(22)出願日　平成７年(1995)２月16日

(71)出願人　000006208
三菱重工業株式会社
東京都千代田区丸の内二丁目５番１号

(72)発明者　加藤　聖樹
兵庫県高砂市荒井町新浜二丁目１番１号
三菱重工業株式会社高砂研究所内

(72)発明者　藤田　一郎
兵庫県神戸市兵庫区和田崎町一丁目１番１号　三菱重工業株式会社神戸造船所内

(72)発明者　山本　公之
兵庫県神戸市兵庫区和田崎町一丁目１番１号　三菱重工業株式会社神戸造船所内

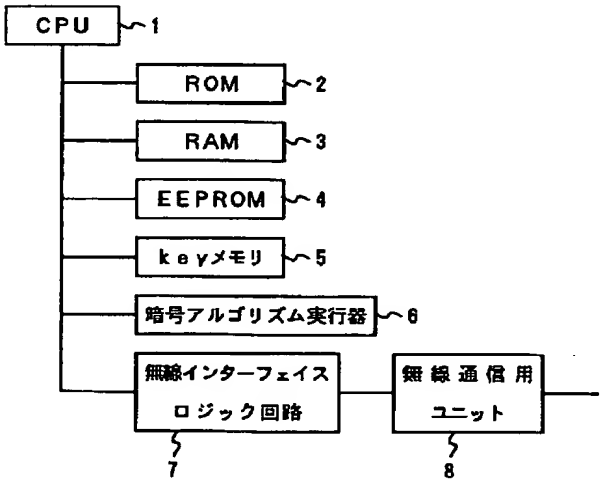
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　非接触ＩＣカードシステム

(57)【要約】

【目的】本発明は、地上機アンテナとの無線回線上のセキュリティを守ることができる非接触ＩＣカードシステムを提供することを目的とする。

【構成】本発明に係る非接触ＩＣカードシステムは、有料自動車道路をノンストップかつキャッシュレスで通行できる料金収受システムの非接触ＩＣカードシステムにおいて、非接触ＩＣカード１１は、メッセージ暗号化のための暗号アルゴリズム実行器６と、暗号化のための機密キー格納メモリ５により構成され、地上機アンテナ１４も、暗号アルゴリズム実行器６と、暗号化のための機密キー格納メモリ５により構成されることにより、非接触ＩＣカード１１と機上機アンテナ１４の双方から発信されるメッセージを暗号化し、キー番号９も同時にメッセージの内容として発信し、メッセージごとに暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。



1

【特許請求の範囲】

【請求項１】　有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ＩＣカードシステムにおいて、（Ａ）非接触ＩＣカード（１１）は、メッセージ暗号化のための暗号アルゴリズム実行器（６）と、暗号化のための機密キー格納メモリ（５）により構成され、（Ｂ）地上機アンテナ（１４）も、暗号アルゴリズム実行器（６）と、暗号化のための機密キー格納メモリ（５）により構成されることにより、（Ｃ）非接触ＩＣカード（１１）と機上機アンテナ（１４）の双方から発信されるメッセージを暗号化し、（Ｄ）キー番号（９）も同時にメッセージの内容として発信し、（Ｅ）メッセージごとに、暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする非接触ＩＣカードシステム。

【請求項２】　有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ＩＣカードシステムにおいて、（Ａ）非接触ＩＣカード（１１）は、メッセージ暗号化のための暗号アルゴリズム実行器（１０６）と、暗号化のための機密キー格納メモリ（１０５）と、ランダムナンバー発生器（１０７）により構成され、（Ｂ）地上機アンテナ（１４）も、暗号アルゴリズム実行器（１０６）と、暗号化のための機密キー格納メモリ（１０５）と、ランダムナンバー発生器（１０７）により構成されることにより、（Ｃ）ランダムナンバー発生器（１０７）で乱数を発生させ、（Ｄ）前記ランダムナンバーと任意に選択したマスターキー（１１３）により、暗号化関数を実行して、一時キーを作成し、（Ｅ）前記一時キーと、非接触ＩＣカード（１１）と地上機アンテナ（１４）の双方から発信させるメッセージを暗号化し、（Ｆ）さらに選択したキー番号と乱数も同時にメッセージの内容として発信し、（Ｇ）メッセージごとに、暗号化のためのキーと乱数を更新することにより、交換されるメッセージの機密性を向上させることを特徴とする非接触ＩＣカードシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、有料道路の料金収受に利用される非接触ＩＣカードシステムに関する。本発明は、上記以外にも物流・入退出管理システムなど、特にセキュリティが要求される分野にも利用することができる。

【０００２】

【従来の技術】近年、有料道路での交通渋滞緩和・料金収受業務の省力化の一案として非接触ＩＣカードシステムの実用化研究が盛んに実施されている。図６は、近年の非接触ＩＣカードシステムの運用メッセージを示したものである。図６において、１１は非接触ＩＣカードを

2

示したものであり、車両１２に搭載されて、非接触ＩＣカードシステム使用可能な料金所ゲートに進入する事になる。

【０００３】１４は地上機アンテナであり、筐体１５に支持されている。１３は地上機アンテナが作り出す非接触ＩＣカードとの無線による通信領域である。

【０００４】１６は地上機アンテナを制御する、アンテナ制御装置である。１７は料金所ブースである。このような、非接触ＩＣカード使用可能な料金所ゲートに車両１２が進入した場合、非接触ＩＣカードは、地上機アンテナが出力する問合せメッセージに応答して、固有情報を地上機アンテナに返信することになる。

【０００５】この固有情報の中には、非接触ＩＣカードのＩＣ番号や、車種区分、入口料金所の情報などの重要なデータを含んでいる。地上機アンテナおよびアンテナ制御装置では、その情報を受信し、課金値（通行料金）を計算し、非接触ＩＣカードに返送することになる。

【０００６】非接触ＩＣカードでは、その課金値を受信し、内部の記録媒体から課金値を減算し、新残額に更新することになる。図７は、従来の非接触ＩＣカードの内部ブロック図を示したものである。図７において、２２０は非接触ＩＣカードのＣＰＵである。

【０００７】２２１はプログラム用のＲＯＭ、２２２は作業用もしくは、データ一時記憶用のＲＡＭである。２２３は、金額を電気的に記憶するＥＥＰＲＯＭである。

【０００８】２２４は、無線通信用で受信したシリアルデータをパラレルデータに変換したり、ＣＰＵのデータを無線通信用に加工したりする無線通信用ロジックである。２２５は、無線通信のためのアナログユニットであり、データ復調回路、データ変調回路などより構成されている。

【０００９】

【発明が解決しようとする課題】ところが上記、従来の非接触ＩＣカードでは、非接触ＩＣカードと地上機アンテナとの無線回線上のセキュリティは、何ら考慮されていなかった。つまり、地上機から送信される問合せメッセージも、課金処理メッセージも、非接触ＩＣカードから返送されるＩＤメッセージもすべて、一般的に知識のある人が認識可能なメッセージ（平文）でやりとりされていた。

【００１０】このような事態は、金額情報を扱う料金所システムにおいては、懸念されるべきである。なぜならば、このメッセージの盗聴者は、容易にこのメッセージを理解でき、もし意図すれば、メッセージの一部を、有利なメッセージに交換したりして、正常の課金値よりも格安でもしくは、無料で料金所ゲートを通過することも可能である。本発明は、これらの問題を解決することができる非接触ＩＣカードシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

（第１の手段）本発明に係る非接触ＩＣカードシステムは、有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ＩＣカードシステムにおいて、（Ａ）非接触ＩＣカードは、メッセージ暗号化のための暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリにより構成され、（Ｂ）地上機アンテナも、暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリにより構成されることにより、（Ｃ）非接触ＩＣカードと機上機アンテナの双方から発信されるメッセージを暗号化し、（Ｄ）キー番号も同時にメッセージの内容として発信し、（Ｅ）メッセージごとに、暗号化のためのキーを更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。

（第２の手段）本発明に係る非接触ＩＣカードシステムは、有料自動車道路を、ノンストップかつキャッシュレスで通行できる料金収受システムの非接触ＩＣカードシステムにおいて、（Ａ）非接触ＩＣカードは、メッセージ暗号化のための暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリと、ランダムナンバー発生器により構成され、（Ｂ）地上機アンテナも、暗号アルゴリズム実行器と、暗号化のための機密キー格納メモリと、ランダムナンバー発生器により構成されることにより、（Ｃ）ランダムナンバー発生器で乱数を発生させ、（Ｄ）前記ランダムナンバーと、任意に選択したマスターキーにより、暗号化関数を実行して、一時キーを作成し、（Ｅ）前記一時キーと、非接触ＩＣカードと地上機アンテナの双方から発信させるメッセージを暗号化し、（Ｆ）さらに、選択したキー番号と乱数も同時にメッセージの内容として発信し、（Ｇ）メッセージごとに、暗号化のためのキーと乱数を更新することにより、交換されるメッセージの機密性を向上させることを特徴とする。

【００１２】

【作用】

（請求項１に係る発明の作用）本発明の非接触ＩＣカードシステムによれば、地上機アンテナからのメッセージには先頭にキー（以下Ｋｅｙという）番号が付加されている。

【００１３】その後に続くデータは、このＫｅｙ番号で指定された機密Ｋｅｙで暗号化されている。非接触ＩＣカードでは、この機密メッセージを受信すると、最初にＫｅｙ番号を認識し、このＫｅｙ番号で指定された機密ＫｅｙをＫｅｙメモリの中から検索し、暗号アルゴリズム実行器に入力する。

【００１４】この暗号アルゴリズム実行器に、同時に受信した機密データを入力することにより出力として、平文の認識可能なメッセージを得ることができる。非接触ＩＣカードが地上機アンテナに返信する際も同様である。

【００１５】非接触ＩＣカードは、任意にＫｅｙメモリのなかから機密Ｋｅｙを選択し、そのＫｅｙでデータを暗号化して、そのＫｅｙのインデックスであるＫｅｙ番号とともに地上機に返信する。

（請求項２に係る発明の作用）本発明の非接触ＩＣカードシステムによれば、地上機アンテナからのメッセージには先頭にＫｅｙ番号が付加されている。

【００１６】その後、数バイトは乱数が発信される。更にその後に続くデータは、このＫｅｙ番号で指定された機密Ｋｅｙと乱数を暗号化関数で実行した一時Ｋｅｙで暗号化されている。

【００１７】非接触ＩＣカードでは、この機密メッセージを受信すると、最初にＫｅｙ番号を認識し、このＫｅｙ番号で指定された機密ＫｅｙをＫｅｙメモリの中から検索し、暗号アルゴリズム実行器に入力する。

【００１８】次に、受信された乱数を同時に暗号アルゴリズム実行器に入力し、出力として一時Ｋｅｙを得る事ができる。その後、この一時Ｋｅｙと、同時に受信した機密データを、再び暗号化アルゴリズム実行器に入力することにより、出力として、平文の認識可能なメッセージを得ることができる。

【００１９】非接触ＩＣカードが地上機アンテナに返信する際も同様である。非接触ＩＣカードは、任意にＫｅｙメモリのなかから機密Ｋｅｙを選択し、更に乱数を発生させ、暗号化アルゴリズム発生器に入力し、一時Ｋｅｙを作成する。そのＫｅｙでデータを暗号化して、もともとの機密ＫｅｙのＫｅｙ番号と、数バイトの乱数とともに地上機に返信する。

【００２０】

【実施例】

（第１実施例）本発明の第１実施例を図１、図２を用いて説明する。図１において、１は非接触ＩＣカードのＣＰＵである。

【００２１】２はプログラム用のＲＯＭである。３は、ＣＰＵの作業用ＲＡＭであり、同時にデータの一時格納エリアでもある。

【００２２】４は不揮発性のメモリ（ＥＥＰＲＯＭ）であり、非接触ＩＣカードが前払い形態の運用をされた場合、電気的に金額を記憶する財布代わりになるものである。５はＫｅｙメモリであり、複数の暗号Ｋｅｙが格納された領域である。

【００２３】６は暗号アルゴリズム実行器である。７は無線インタフェースロジック回路であり、８は無線通信用ユニットである。

【００２４】本発明の、非接触ＩＣカードと地上機アンテナで双方に交信されるメッセージは、図２のようになっている。基本構成は、暗号化の際に使用されたＫｅｙを指し示すＫｅｙ番号（Ｋｅｙインデックス）９と、そのＫｅｙで暗号化された機密データ１０の集まりで１つ

のパケットが構成される事になる。

【００２５】まず、地上機は、このパケットを非接触ＩＣカードに送信することになる。これを受信した非接触ＩＣカードでは、まずＫｅｙ番号の認識を行なう。そして、このＫｅｙ番号が示すＫｅｙの内容を、暗号アルゴリズム実行器に入力すると同時に、受信した暗号化されたメッセージも一緒に入力する。その出力として平文の認識可能なデータを得ることができるようになる。このような暗号化されたデータから元の平文を再生する動作を復号処理と呼ぶ。

【００２６】つまり、地上機のアンテナ制御装置と非接触ＩＣカードの双方で、同じ暗号Ｋｅｙをもっていなければ、暗号化されたメッセージの解読はできない事になる。これは、この暗号化Ｋｅｙを知り得ない外部の盗聴者から重要データを保護するごとに非常な有効な手段となる。

【００２７】さらに、非接触ＩＣカードが、地上機アンテナに対して返信する場合も同じであり、まず最初に非接触ＩＣカードは、任意のＫｅｙ番号を選択し、そのＫｅｙで示されたＫｅｙメモリの内容、すなわち暗号Ｋｅｙ自体を、暗号アルゴリズム実行器に入力する。

【００２８】それと同時に、送信したいメッセージも一緒に、暗号アルゴリズム実行器に入力する。その結果として、機密Ｋｅｙで暗号化されたメッセージをえる事ができる。このように、解読可能な平文から機密Ｋｅｙを用いてメッセージを暗号化する動作を、暗号処理と呼ぶ。

【００２９】そして、その任意のＫｅｙと暗号化されたデータをパケットにして、地上機アンテナに返信する事になる。

（第２実施例）本発明の第２実施例を図３、図４および図５を用いて説明する。

【００３０】図３において、１０１は非接触ＩＣカードのＣＰＵである。１０２はプログラム用のＲＯＭである。１０３は、ＣＰＵの作業用ＲＡＭであり、同時にデータの一時格納エリアでもある。

【００３１】１０４は不揮発性のメモリ（ＥＥＰＲＯＭ）であり、非接触ＩＣカードが前払い形態の運用をされた場合、電気的に金額を記憶する財布代わりになるものである。

【００３２】１０５はＫｅｙメモリであり、複数の暗号Ｋｅｙが格納された領域である。１０６は暗号アルゴリズム実行器である。１０７はランダムナンバー発生器である。

【００３３】１０８は、無線インタフェースロジック回路であり、１０９は無線通信用ユニットである。これらの一時Ｋｅｙ作成過程とデータの暗号化過程を示したものが図４である。図４に示すように、非接触ＩＣカードは最初に、自身でランダムナンバーを発生させる。

【００３４】そのランダムナンバーと、任意に選択した機密Ｋｅｙ（マスターＫｅｙ）を同時に暗号アルゴリズム実行器に入力する。その結果として、一時Ｋｅｙを得る事ができる。

【００３５】次に、その一時Ｋｅｙと、暗号化したい（被暗号化）データを、同時に暗号アルゴリズム実行器に入力する。その結果として暗号化された機密データを得る事ができるようになる。

【００３６】本発明の、非接触ＩＣカードと地上機アンテナの双方に交信されるメッセージは、図５の示すようになっている。基本構成は、暗号化の際に使用されたＫｅｙを指し示すＫｅｙ番号（Ｋｅｙインデックス）１２０と、そのＫｅｙとランダムナンバー１２１で暗号化関数により作成された一時Ｋｅｙと、さらにその一時Ｋｅｙで暗号化された機密データ１２２の集まりで、１つのパケットが構成される事になる。

【００３７】実際のアプリケーションでは、以下のように使用される事になる。まず、地上機は、このパケットを非接触ＩＣカードに送信することになる。これを受信した非接触ＩＣカードでは、まずＫｅｙ番号の認識を行なう。

【００３８】そして、このＫｅｙ番号が示すＫｅｙの内容を、暗号アルゴリズム実行器に入力すると同時に、受信したランダムナンバーも一緒に入力する。その出力として一時Ｋｅｙを得ることができる。

【００３９】この一時Ｋｅｙと、受信された機密データを、再度、暗号アルゴリズム実行器に入力することにより、平文の認識可能なデータを得ることができるようになる。このような暗号化されたデータから元の平文を再生する動作を復号処理と呼ぶ。

【００４０】つまり、地上機のアンテナ制御装置と非接触ＩＣカードの双方で、同じ暗号Ｋｅｙをもっていなければ、暗号化されたメッセージの解読はできない事になる。これは、この暗号化Ｋｅｙを知り得ない外部の盗聴者から重要データを保護することに非常な有効な手段となり得る。

【００４１】さらに、非接触ＩＣカードが、地上機アンテナに対して返信する場合も同じであり、まず最初に非接触ＩＣカードは、任意のＫｅｙ番号を選択し、そのＫｅｙで示されたＫｅｙメモリの内容、すなわち暗号Ｋｅｙ自体を、暗号アルゴリズム実行器に入力する。

【００４２】それと同時に、非接触ＩＣカードで発生させたランダムナンバーも入力する。その結果として一時Ｋｅｙを得ることができ、送信したいメッセージとこの一時Ｋｅｙとを再度、暗号アルゴリズム実行器に入力する。

【００４３】その結果として、機密Ｋｅｙで暗号化されたメッセージを得る事ができる。このように、解読可能な平文から機密Ｋｅｙを用いてメッセージを暗号化する動作を、暗号処理と呼ぶ。

【００４４】そして、その任意のＫｅｙと、ランダムナ

ンバーと暗号化されたデータを、パケットにして、地上機アンテナに返信する事になる。なお、発生させるランダムナンバーの長さは、１バイトよりも複数バイトある方が、作成される一時Ｋｅｙの展開が豊富であり、データのセキュリティは更に向上する。

【００４５】

【発明の効果】本発明は前述のように構成されているので、以下に記載するような効果を奏する。

（請求項１に係る発明の効果）

（１）本発明の非接触ＩＣカードシステムによれば、地上機アンテナと交互に交換されるメッセージ内容は、機密Ｋｅｙで暗号化されており、盗聴者がそのメッセージをなんらかの形で傍受できたとしても、機密Ｋｅｙを知り得なければ、有効でかつ意味のあるメッセージに解読できない事になる。

（２）したがって、無線回線上のメッセージのどの部分がどのような意味をなすものなのかを認識する事ができない事になり、その部分をすり替えて、不正に通行料金をごまかそうという行為など、あらゆる不正を防止することができる。

（３）また、本発明の最も効果的な使用方法は、交信されるメッセージ毎に、暗号化のＫｅｙ、すなわちＫｅｙ番号を変化させることである。

【００４６】これにより、暗号化されたメッセージが幾重にも違った形に展開でき、さらに解読を困難にすることができるようになる。

（請求項２に係る発明の効果）

（１）本発明の非接触ＩＣカードシステムによれば、地上機アンテナと交互に交換されるメッセージ内容は、機密Ｋｅｙと、ランダムナンバーで、暗号化されており、盗聴者がそのメッセージをなんらかの形で傍受できたとしても、機密Ｋｅｙを知り得なければ、有効でかつ意味のあるメッセージに解読できない事になる。

（２）したがって、無線回線上のメッセージのどの部分が、どのような意味をなすものなのかを認識する事ができない事になり、その部分をすり替えて、不正に通行料金をごまかそうという行為など、あらゆる不正を防止することができる。

（３）また、本発明の最も効果的な使用方法は、交信されるメッセージ毎に、暗号化のＫｅｙ、すなわちＫｅｙ番号を変化させ、更にランダムナンバーで一時的なＫｅｙをえることである。

【００４７】これにより、一時Ｋｅｙも、暗号化されたデータも、無数の広がりをみせ、暗号化されたメッセージが幾重にも違った形に展開でき、さらに解読を困難にすることができるようになる。

【図面の簡単な説明】

【図１】本発明の第１実施例に係る非接触ＩＣカードの構成図。

【図２】本発明の第１実施例に係るパケットの構成図。

【図３】本発明の第２実施例に係る非接触ＩＣカードの構成図。

【図４】本発明の第２実施例に係る暗号化処理ルーチン。

【図５】本発明の第２実施例に係るパケットの構成図。

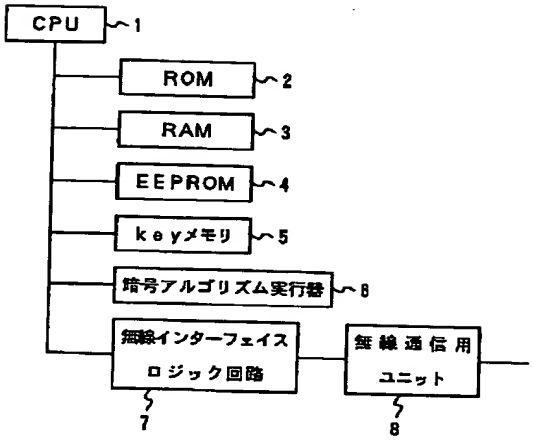
【図６】非接触ＩＣカードの運用イメージ図。

【図７】従来の非接触ＩＣカードの構成図。

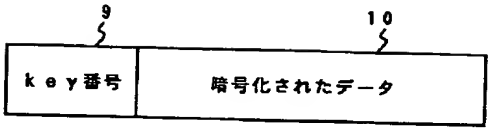
【符号の説明】

１…ＣＰＵ、
２…ＲＯＭ、
３…ＲＡＭ、
４…ＥＥＰＲＯＭ、
５…Ｋｅｙメモリ、
６…暗号アルゴリズム実行器、
７…無線インタフェースロジック回路、
８…無線通信ユニット、
９…Ｋｅｙ番号、
１０…暗号化されたデータ、、
１１…非接触ＩＣカード、
１２…車両、
１３…地上機アンテナが作り出す無線による通信領域、
１４…地上機アンテナ、
１５…筐体、
１６…地上機のアンテナ制御装置、
１７…料金所ブース、
１０１…ＣＰＵ、
１０２…ＲＯＭ、
１０３…ＲＡＭ、
１０４…ＥＥＰＲＯＭ、
１０５…Ｋｅｙメモリ、
１０６…暗号アルゴリズム実行器、
１０７…ランダムナンバー発生器、
１０８…無線インタフェースロジック回路、
１０９…無線通信ユニット、
１１３…マスターＫｅｙ、
１２０…Ｋｅｙ番号、
１２１…ランダムナンバー、
１２２…暗号化されたデータ。
２２０…ＣＰＵ、
２２１…ＲＯＭ、
２２２…ＲＡＭ、
２２３…ＥＥＰＲＯＭ、
２２４…無線インタフェースロジック回路、
２２５…無線通信ユニット。

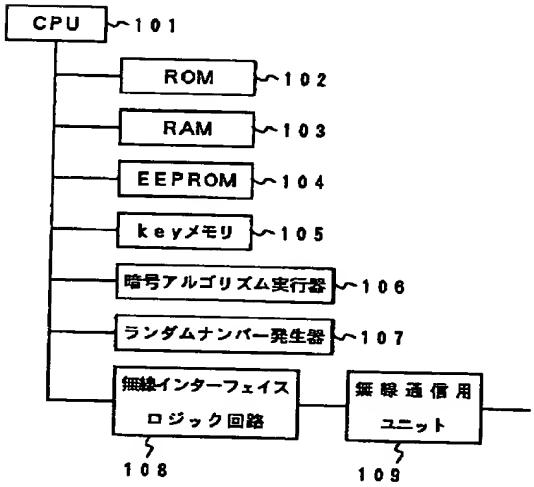
【図１】



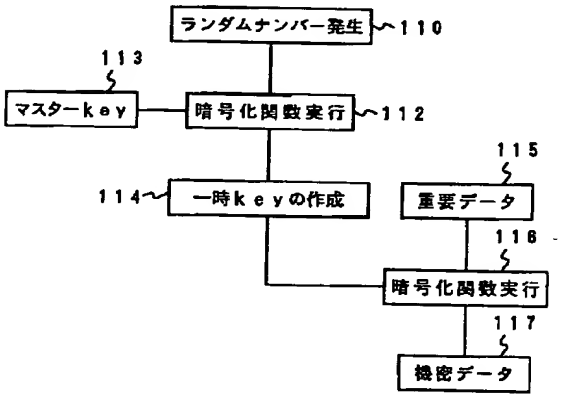
【図２】



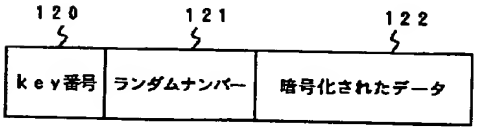
【図３】



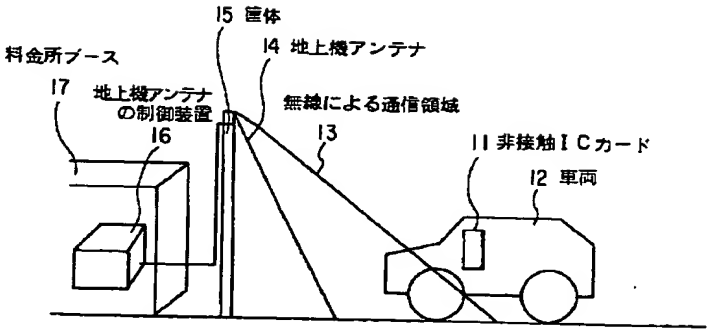
【図４】



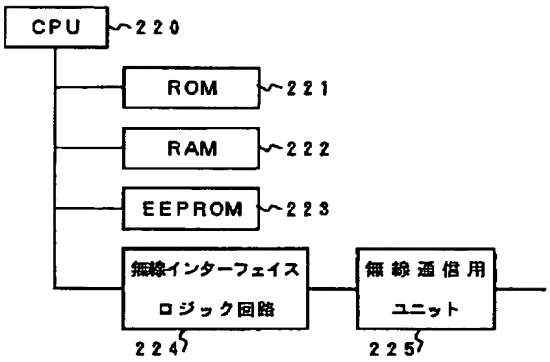
【図５】



【図６】



【図７】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
G07F	7/08			G08G	1/017		
G08G	1/017			G07F	7/08	S	